

TRM Glossary

Version 3.0

#

3GL (third-generation language) – is a high-level programming language such as FORTRAN, COBOL, BASIC, Pascal or C, which compiles to machine language.

4GL (fourth-generation language) – is a high-level language suitable for end-user or programmer data access and capable of reasonably complex data manipulation. It includes two categories of software development tools: application generators for production applications, and information generators for decision-support applications. 4GLs are relatively nonprocedural and easier to use than 3GLs (e.g., COBOL, FORTRAN and C), but are less powerful and more wasteful of computer resources. Generally, three types of 4GL are recognized:

- A procedural language integrated with a database management system. Examples include Ideal (Computer Associates) and Natural (Software AG)
- An information generator. Examples include FOCUS (Information Builders), Nomad 2 (Must Software) and Ramis (Computer Associates)
- A code generator or nonprocedural tool. Examples include SQLForms (Oracle) and Telon (Computer Associates). These tools are also called lower-CASE tools.

3270 – IBM's interactive communications terminal standard used to communicate with an IBM mainframe or compatible system.

A

ActiveX – A set of technologies from Microsoft provides tools for linking desktop applications to the World Wide Web. Enabled using a variety of programming tools including Java, Visual Basic, and C++.

Adaptive/Assistive Technologies (AAT) – provide access to systems and applications for users with communication, physical access, or learning disabilities.

American National Standards Institute (ANSI) – a private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

Application – A set of coded instructions that direct a computer to perform desired functions. The term is sometimes used in place of “application program,” “software”, or “program,” which are used to process data for the user. Applications can be custom-written or purchased.

Application Architecture – The Application Architecture is the focal point of an organization’s systems inventory. It defines how applications are designed, how they cooperate, and where they reside. Good application architectures will enable a high level of distributed system integration, reuse of components, rapid deployment of applications and high responsiveness to changing business requirements.

Application layer – The software that “runs” on top of the system services layer.

An **Application Programming Interface (API)** is software, either custom or COTS, that uses a specific implementation to exchange data with another system. Business rules provide the specific interaction mechanism. Each reusable component requires a properly documented API. An API is the specific method prescribed by a computer operating system or by another application program by which a programmer writing an application program can make requests of the operating system or another application. A set of calling conventions that defines how a service is invoked through software. An interface that enables programs written by users or third parties to communicate with certain vendor-supplied software. (1) a documented set of instructions by which a program can invoke the functions of a system, such as a DBMS or a transaction processing monitor, (2) used to integrate two different application programs, at least to the extent of allowing them to share data.

Application Software – A program that performs a task or process specific to a particular end-user’s needs, or solves a particular problem. Enterprise applications are typically large-scale business systems that organizations use to manage their operations.

Architecture – A structured set of protocols that implements a system’s functions. A network architecture defines the functions, formats, interfaces, and protocols required for end users to exchange information.

Architecture Exception – The process whereby the appropriate governance body reviews line-of-business or IT project request for an exception to the architecture and formally arbitrates disputes arising from the Architecture Review process.

Architecture Management Processes – The collection of processes employed to ensure that the appropriate activities occur so that an organization’s architecture is developed and refreshed on a regular basis, and that IT projects and initiatives comply with the preferred direction set forth in the architecture documentation. The basic processes that compose Architecture Management are: Architecture Development and Renewal, Architecture Domain Team Chartering, Architecture Communications, Architecture Research, Architecture Review and Architecture Exception.

Architecture Principle(s) – General philosophical statements that apply to the design and implementation of systems and applications within the various IT architectures covered in the IEA Technical Reference Model. Usually expressed as descriptive statements about the desirable

characteristics of a particular architectural element. For example, “Effective interfaces and applications appear and behave in ways that are consistent with users’ expectations”.

Architecture Review – The formal process of evaluating the extent to which a system proposed for development and deployed in the organization’s technology environment conforms to the technology architecture and that the total cost of ownership for a given proposed system is adequately determined and known to all stakeholders.

Asynchronous – In computer programming, asynchronous (from Greek meaning "not at the same time" and pronounced "ay-SIN-kro-nus") pertains to processes that proceed independently of each other until one process needs to "interrupt" the other process with a request. Using the client-server model, the server handles many asynchronous requests from its many clients. The client is often able to proceed with other work or must wait on the service requested from the server.

Authentication – The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

Authorization – The process of giving someone permission to do or have access to something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth).

B

Bandwidth – Data/voice/video carrying capacity of a transmission medium, usually measured in hertz (Hz).

With **Binary Compatibility**, there is no need to recompile an application for different platforms. For example, if an application is going to be deployed on servers located in State Offices, all servers running that application should be binary compatible – this must be ensured even if the platforms are from the same manufacturer. The platforms must run the same version of the operating system and must not require any recompilation of business applications so that deployment throughout the various offices means a simple copy of a program from one office to another. Total binary compatibility will support automated software distribution across servers, which will reduce support costs and provide stable computing platforms that can be reliably shared and moved across the Bureau. Technologies like the Java Virtual Machine and Java servlets fit this definition of binary compatibility, but may not fit every situation due to compromised performance.

BIND – is a cross-platform, open source nameserver that follows the standards defined in the RFCs related to DNS.

Bus – (1) A high-speed physical transmission path or channel. Typically an electrical connection with one or more conductors, wherein all attached devices receive all transmissions at the same time. (2) Local network topology, such as that used in Ethernet and the token bus, where all network nodes listen to all transmissions, selecting certain ones based on address identification. It involves some type of contention-control mechanism for accessing the bus transmission medium.

Business Architecture – This architecture identifies business systems and their interactions in order to:

- Drive the strategic decisions in the technology architecture.
- Identify business services independent of application-specific invocations of those services.
- Understand how and what data are strategic to the enterprise.
- Provide the basis for the strategic applications of information technology.

Business Driver – A collective term that is used to describe the various influencing factors that cause (directly or indirectly) changes in an enterprise's business processes, including external forces (changes in competition/market, globalization, economy, customers, regulation, politics, and technology) and responses to these forces (including business strategies, goals, objectives, requirements, and strategies).

Business Function – A logical grouping of functionality used to support execution of Business Processes.

Business Information Requirements – The information needs of an enterprise that result from business drivers, and/or their corresponding business strategies. Can be identified at a high level by asking: What information is needed? Where does the information come from? Who needs it? When do they need it?

Business Intelligence Tools – Employed by end users for decision-making and analytical processes. These tools allow the users to dynamically query the data and information stored in data warehouses. They provide query, reporting, graphing, trend analysis, calculating, and summarizing capabilities. Business intelligence tools provide the ability to analyze and access data contained in the data warehouse. Typically, several tools are selected within an organization, based on the function needed.

Business Logic – The rules that control how to complete a task or step in a work process. For example, application logic that governs processing a payment or address change. These applications are often transactional in nature – resulting in database/file updates.

Business Process – A collection of business activities (tasks) that transform input(s) into output(s) of value to the Enterprise.

Business Rules – Requirements and specifications for the line-of-business decision-making process. Most business rules are declarative. Business rules serve to constrain, define, and assert how business will be transacted. Business rules also define actions to be taken in a specific circumstance.

Business Strategy – The planned approach to achieving an enterprise's business drivers.

C

Calendaring and Scheduling (C & S) – A technology that, by combining with an organization's overall groupware system(s), provides a methodology for the coordination and communication of individual and group activities and plans. Time-management functions that schedule events (such as meetings, lectures, and conferences) and access (and manage) calendric information about people, facilities, and equipment.

Calendar Store – A database storing C & S information and schedules. The database may reside on a single server, or may be distributed across multiple servers over the network.

Capability Maturity Model (CMM) – The Software Engineering Institute's (SEI's) Capability Maturity Model (and the SCE process based on it) offers an initial basis for defining software development processes for regulatory purposes.

C & S Client – The front-end user interface of the C & S application that runs on the user's desktop. It allows users to view and manipulate their calendar and schedule information, and to coordinate and schedule meetings from their desktop computer.

C & S Server – The hardware and software that provides calendaring and scheduling services to C & S clients. It manages calendar and schedule information, and the exchange of C & S information between C & S users. The Calendar store is managed by the C & S server.

Change Management – Process of planning, controlling, and managing enterprise changes.

Classification – A method for grouping similar or like things. In the IEA, industry standards and technology products are grouped into lifecycle classifications that reflect their suitability for use at Interior.

Client – A system or a program that requests the activity of one or more other systems or programs, called servers, to accomplish specific tasks. In a client/server environment, the workstation is usually the client. The client serves as a user interface, as well as a processor for many time-consuming tasks, allowing the server to devote itself to central storage and other tasks.

Client/Server – (1) In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client and the answering program is called a server. (2) In Information Resource Management, a computing model where functionality is divided between software clients and software servers. Clients depend on the services provided by servers such as another application, component, or database to complete the intended function. (3) A technical architecture that links workstations into networks, enabling increased productivity by means of

sharing information. Individual users, or “clients,” are “served” over a network by a central machine that acts as a common repository of information and programs.

Commercial off-the-shelf (COTS) application – Also known as COTS software.

Common Gateway Interface (CGI) – A data-passing specification used when a Web server must send or receive data from an application such as a database. A CGI script passes the request from the Web server to a database, gets the output, and returns it to the Web client.

Common Internet File system – The common Internet file system uses the server message block protocol (SMB) for sharing disk space from one system among other systems.

Compatibility – The ability of two devices to communicate with each other understandably, or the ability of software to run on a particular hardware platform.

The **Common Internet File System (CIFS)** uses the server message block protocol (SMB) for sharing disk space from one system among other systems.

Common Management Information Protocol (CMIP) – The Open Systems Interconnection (OSI) protocol for the exchange of network management information.

A **Component** – is a piece of software or hardware that is designed to fulfill a single purpose and to interoperate with other components.

Component Object Model (COM) – A framework developed by Microsoft that supports interoperability and reusability of distributed objects by allowing developers to build systems by assembling reusable components from different vendors.

Conceptual Architecture – A principles-based, enterprise-level layer of a technical architecture to ensure clear decisions to sub-optimize individual components in order to optimize total effectiveness of the overall enterprise architecture to enable business strategies.

Content Management – Tools used for managing the versioning, workflow, and deployment of web content.

Control Layer – The layer(s) in an application that control various aspects of the application functionality. It is a way to externalize the ordering or flow of functionality independent of the actual business logic. This ensures that the business logic can be easily adapted, reordered, or reorganized in order to meet changing business needs by changing the control not the actual business logic.

Cookie – A chunk of information that is passed from one application to another, with the expectation that the receiver will store the chunk and send it back later. The most common usage for cookies is to save state in client/server applications, track user information, and provide a user customizable experience.

Corporate Metadata Repository (CMR) – 1) A repository that contains metadata, which is information about data (for example, shared data definitions, data aliases, and where OLTP and OLAP data can be found). A data repository is an important aspect of a successful data warehouse effort because it contains all the information about the data and processes used to populate and access a data warehouse. 2) The corporate metadata repository provides a single enterprisewide source for data definitions. This tool becomes more important in the XML/EDI world because data structure, definition and context are important for data integration. The CMR is the local place to maintain data type definition files.

CORBA (Common Object Request Broker Architecture) – An Object Management Group (OMG) interoperability standard for object-oriented applications communicating within heterogeneous environments.

D

Data Access Middleware – The communications layer between data access programs and tools and databases. Data access middleware is designed to enable communication between a data access programming tier and a database, as opposed to application communication middleware, which enables communication between the programming tiers of an N-tier application system.

Data Administration – Technologies/strategies for facilitating the design of maintaining and administering the data in a DBMS.

Database – A collection of structured data that is application-independent.

Database Access Tools – Used to query and retrieve data from existing databases and write reports. These tools can be provided either through a purchased package or integrated with EIS and DSS applications by application developers. Some examples of these tools are Microsoft Access, Microsoft Excel, Lotus 1-2-3, and custom-written programs using ODBC and SQL. Data is organized and managed through a database management system (DBMS). The database organization can be relational or nonrelational.

Data Management Architecture – The Data Management Architecture defines the mechanics for managing, securing, and maintaining the integrity of an enterprise's significant logical entities. These entities must be recorded and accounted for in a business information environment. The architecture provides standards for accessing data, and, if appropriate, business objects.

Database Management System (DBMS) – Manages data storage, structure, access, and security. Fields can be indexed to improve the performance of queries against the data, a system comparable to that of a dictionary that has tabs for the letters of the alphabet so that it is easier to look up a word, or to a reference book, which has an index to quickly find information needed. The following are types of DBMSs.

- **Relational Database Management System (RDBMS)** – Software designed to manage the collection of data. Data is organized into related tables so that

relationships between data can be established. Relational databases can contain normalized data. Normalized data is organized so that unique data is stored only one time, instead of multiple times for each table (e.g., a non-normalized database). A relationship is established between the unique data and its related information.

- **Object Database Management System (ODBMS)** – Objects provide a rich model for capturing business complexity. Objects can represent complete business entities and the relationships between them. They are easily extensible as business processes change and fit well in a networked application architecture. ODBMSs integrate database functionality with object programming languages. The ODBMS extends an object-oriented programming language with persistent data, concurrency control, data recovery, and associative queries.
- **Multidimensional Database Management System (MDDBMS)** – Specifically designed for efficient storage and retrieval of large volumes of data. Data is stored similar to the way it is in a spreadsheet, so it is easier for end users to understand and manipulate. Multidimensional databases store data that is closely related and stored, viewed, and analyzed from multiple perspectives (i.e., dimensions). Multidimensional databases are sometimes referred to as post-relational databases or a more advanced form of object-oriented database.

Data Bus – Software equivalent of a hardware bus. Applications attach to a data bus with a known address. Applications can send and receive data on the data bus by using the addresses of the other applications attached. MQSeries from IBM is an example of data bus technology. Regardless of the underlying network protocol, data bus products are packet or message oriented.

Data Cleansing – Technologies used to enhance the integrity and validity of the data in a DBMS.

Data Dictionary – A collection of descriptions of the data objects or items in a data model for the benefit of programmers and others who might need to refer to them.

Data Integrity – Accuracy, validity, and consistency of data, maintained according to a set of rules for modifying a database

Data Mart – A subset of a data warehouse. Where data warehouses are designed to support many requirements for multiple business needs, data marts are designed to support specific requirements for specific Decision Support System (DSS) applications (i.e., particular business needs). Although a data mart is a subset of a data warehouse, it is not necessarily smaller than a data warehouse. Specific DSS needs may still require large amounts of data. Data marts are typically considered a solution for distributed users who want exclusive control of the information required for their business need.

Data Migration Tool – Copies selected data from legacy and other OLTP systems. Data transformation reformats extracted data according to metadata definitions and puts it into a data warehouse. Extraction and transformation tools are required to integrate data from multiple sources and to ensure consistency of information derived from data created in a complex, heterogeneous OLTP environment.

Data Mining – Used to analyze the data stored in data warehouses. It can provide valuable insights into the business. Data mining scans large amounts of data stored in data warehouses to reveal patterns or correlations.

Data Model – Specifies the data formats and the relationships of fields and tables in an application system. It drives basic database design.

Data Replication Tools – For distributed or remote users, there is sometimes a need to distribute data from a data warehouse to various data warehouses and data marts throughout the organization. When warehouse data is needed for distributed OLAP processing, it can be distributed through a replication service. Replication allows data to be located close to the business users, thus improving performance. This is particularly useful for eliminating latency problems in distributed systems (e.g., WAN) and for access speed with large geospatial databases.

Data Scrubbing Tools – Validate and cleanse data so that its format is consistent and it is accurate, complying with metadata definitions. Data scrubbing is typically performed periodically to ensure that data meets the metadata standards that have been set. It is also performed when data has been loaded into a data mart or data warehouse. For data scrubbing to be successful, data scrubbing tools and defined roles, responsibilities, and procedures are needed. Data scrubbing is needed at multiple levels, including the data entry level in OLTP applications and the data extraction and transformation levels. Data can become “dirty” for many reasons. For example, consider a data entry application that has an open text field called “Description.” If no limitations are placed on the entry of data in that field, end users can type anything in that field, including misspelled words or multiple text descriptions for the same data element.

Data Steward – The person or group of people responsible for implementation of data from a technical perspective including data design, processing of data into the physical platform and managing the data availability, integrity and security according to business requirements.

A **Data Store** contains data. A data store will most likely take the form of a relational database management system (RDBMS). Other data store implementations can be hierarchical, object, and object-relational databases. Indexed sequential access method (ISAM) files is another implementation.

A **Data Type Definition (DTD) file** is used by an XML parser to parse XML data. A DTD allows an application using the DTD to understand an XML data source. A DTD can be defined by a business for its specific needs. This feature provides the business the capability to rapidly change as business needs change.

Data Visualization – is the method of displaying data resulting from end user queries and data mining from a data warehouse in a visual format (i.e., graphs, pie charts, and bar and line charts). Similar to data mining, data visualization can be helpful in realizing trends or patterns in interrelated data.

A **Data Warehouse** stores information compiled from multiple sources and typically is available to people across the organization for analytical processing. It can provide more timely answers to business needs and questions. It is a database for query and analysis, as opposed to a database for processing transactions. Separating the two functions improves flexibility and performance.

Decision Support Systems (DSS) – A computer program application that analyzes business data and presents it so that users can make business decisions more easily. It is an “informational application” (as distinct from an “operational application” that collects the data in the course of normal business operation). A DSS may present information graphically and may include an expert system or artificial intelligence (AI). It may be aimed at business executives or some other group of knowledge workers.

Development Tools – The raw materials by which programmers create custom-built enterprise software.

Directory Services, Message Handling Systems, and Standards – An e-mail system uses directory services, Message Handling Services (MHSs), and standards and protocols to index and manage names, e-mail messages, distribution lists, and devices (including printers and other peripherals, and servers) accessible on networks it serves.

Digital Certificate – The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by trusted third parties known as certification authorities (CAs), such as VeriSign, Inc., after verifying that a public key belongs to a certain owner.

Distributed Component Object Model (DCOM) – Microsoft’s distributed version of Component Object Model (COM), whose version communicates via their version of a remote procedure “call” (RPC).

Distributed Database – Database whose contents (tables, views, columns, files, etc.) reside on more than one system in a network and can be transparently accessed or updated from any system in the network.

Distributed Computing Environment (DCE) – An Open Software Foundation (OSF) initiative to create a vendor-neutral networking and distributed computing environment to support distributed applications, by integrating the appropriate technology or combination of technologies into a single environment while addressing interoperability, standards and security. DCE integrates remote procedure calls, presentation services, a naming directory, security, threads (sequential flows of control similar to tasks), time services (to synchronize clocks) and a distributed file system.

A **Distributed Object** is an object that can be accessed remotely. This means that a distributed object can be used like a regular object, but from anywhere on the network. An object is typically considered to encapsulate data and behavior. The location of the distributed object is not critical to the user of the object. (See Glossary entry for “Object”.)

Distributed Control Systems (DCS) – evolved from centralized process control computers common in the 1960s. The systems were developed for continuous-flow processes that required loop, analog, and limited discrete control. A DCS is a real-time, fault-tolerant system for continuous and complex batch-process applications. Over time, they have evolved from being proprietary hardware and software systems to being UNIX- and Windows NT-based systems.

Distributed Systems Management (DSM) – focuses on the integration of a framework tool such as HP OpenView or Tivoli, in support of the processes and organizational structure of the Bureau's business and IRM requirements.

Document Management System (DMS) – Allows users to store, search, and manipulate documents electronically and maintain a library of text and images in a compact space. Most systems also provide a means for passing documents across a network. A **DMS** manages the processes of authorship, review, editing, production, approval, and delivery of (or access to) large sets of documents throughout an organization.

Documentation – Data that describes code and data. Documentation can be thought of as metadata.

Domain – A related set of technologies.

Domain Architecture – A logical consistent set of principles with rationales and implications, as well as identified industry standards and products that are classified into lifecycle categories.

Domain Layer – Also referred to as "business domain" or "business functionality". This is the layer in an application that contains the collection of services that enforce the business rules, process information, and manage transactions. This layer must be separated from the presentation and the data to truly be effective. This ensures your business rules are not dependent on presentation and data implementations and are easily transportable (or accessible) to any application on any platform.

The **Domain Name System (or "Service") (DNS)** is an important directory standard on the Internet and on local TCP/IP networks. It is used to map the TCP/IP network address of a server (for example, 207.68.156.58) to a better-known form (i.e., www.microsoft.com). The DNS naming convention is used for Internet and e-mail addresses that take the form "name@hostname.organization."

Domain Team – A domain team is responsible for developing architecture principles, with associated rationale and implication, identifying applicable standards and preferred products, and conducting other work assigned by the Architecture Team, for a given collection of related technologies. There is a domain team associated with each of the Technical Architecture Domains

Dynamic Data Exchange (DDE) – A limited method of sharing data between two applications or files. When data is used in both files, with DDE it can be automatically updated in the other.

Both applications must be in use, and DDE does not work over a network. Object Linking and Embedding (OLE) is a more sophisticated development.

E

Electronic Data Interchange (EDI) – is being used to provide an absolute structure to data. For example, bids, order processing, and invoicing data structure are just a few standards defined by EDI. EDI is an absolute standard maintained by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12. There are efforts underway to integrate EDI into XML.

Electronic Forms – Workflow software used to create on-screen data entry forms and provide e-mail routing and tracking of the resulting electronic documents.

Electronic Mail (or “e-mail”) – is the groupware type most critical to the business operations of the Bureau. It enables the fast and efficient exchange of all types of data files across the enterprise. It is able to function during either synchronous or asynchronous interactions. These advantages directly benefit the decision-making process and translate into measurable cost and time savings. The basic characteristics of an e-mail system include features that create, compose, address, send, and receive messages.

Emerging Technologies – New technologies and products that show sufficient promise for future use and should be monitored by the IEA.

End-to-end Services – Offered by the lower three layers of the Open Systems Interconnection (OSI) Reference Model.

End-to-end Storage Management – A component of an overall systems-management infrastructure that improves application availability by reducing the number of storage-related outages and minimizing the length of the outages when they occur.

An **E-mail Client** (also referred to as a Mail User Agent, or MUA) is an application that enables users to compose, send, receive, and organize e-mail. It's called a client because e-mail systems are based on a client-server architecture.

An **E-mail Server** is an applications server that provides services such as files distribution, temporary caching of new messages, and archiving of previously viewed messages. A **message store** is an important subcomponent that resides on the e-mail server. It is a database that enables message-management tasks, such as opening, reading, and deleting messages; and browsing and searching lists of messages. A **directory user agent (DUA)** is another important subcomponent that allows retrieval of information (such as distribution lists and e-mail addresses) from local and network directory services.

An **E-mail Application Programming Interface (API)** allows applications to access the various components of an e-mail system by connecting a sender's e-mail application to a receiver's

application. Using an API, an MUA can manipulate new and stored e-mail messages, create and delete addresses, access and manipulate message components, and authenticate users login in to the e-mail system.

Encryption – A technique of modifying a bit stream of information to make it appear to be a random sequence of bits to someone who does not have access to the encryption scheme.

Enterprise – The highest level of an organization at which common business drivers, strategies and information can be identified.

Enterprise Architecture – Establishes the Agency-wide roadmap to achieve an Agency's mission through optimal performance within an efficient IT environment. Enterprise architectures are “blueprints” for systematically and completely defining an organization's current (baseline) and desired (target) environment.

An **Enterprise Management System (EMS)**, such as Tivoli or CA Unicenter, is a management application that provides a framework in which other tools and third party vendors applications can integrate. The EMS provides a single point of management, and a cohesive view of the network resources.

Enterprise Java Beans (EJB) – The EJB specification defines a way to build server-side, transactional Java-based components. It was developed by Sun Microsystems in collaboration with IBM, Netscape, and Oracle (SINO) and other vendors.

Enterprise Resource Planning (ERP) – Packages that enable the creation of a single corporate image from disparate, decentralized divisions, enabling users to visualize underlying business processes, reshape these processes, and renovate their businesses.

Ethernet – The standard for local communications networks developed jointly by Digital Equipment Corp., Xerox, and Intel. Ethernet baseband coaxial cable transmits data at speeds up to 10 megabits per second. Ethernet is used as the underlying transport vehicle by several upper-level protocols, including TCP/IP.

Executive Information Systems (EISs) – extract data from an enterprise system to provide managers a view of quantitative performance measures on-line. A new generation of systems is meant to provide this information in near-real time, before it's too late to do anything to prevent dysfunctions.

Executive Reporting System (ERS) – A system to generate executive summary reports for Congress, executive management, and oversight groups like the GAO. These reports provide a high-level summary of IEA information.

Extensible – Able to integrate new technology and functionality.

External Systems – Applications of third party business partners that support the organization's business requirements and/or interact with the organization's technology portfolios.

Extract/Transform/Load (ETL) – Technologies used to extract data from source DBMS's, transform the data into an appropriate form, and load it into target Data Marts or Warehouses.

Extranet – Community-of-interest IP networks that provide secure connections between remote users and a main site, or between multiple sites within the same company, including connectivity to business partners, customers, and suppliers.

F

Fax – Communication of a printed page between remote locations. Fax machines scan a paper form and transmit a coded image over the telephone system.

Fiber Optics – A data transmission medium that uses light conducted through glass or plastic fibers. Fiber-optic cables have cores capable of conducting modulated light signals by total internal reflection. Benefits include small diameters, high potential bandwidth, and lower cost than copper.

File Transfer Protocol (FTP) – A system for transferring files between computers over the Internet, Intranet or Extranet.

File-Typing – (used in the Microsoft Windows environment) – File types activate appropriate elements of the Microsoft tool suite, and the tools themselves extend a common set of base classes that help to maintain a high degree of behavioral consistency regardless of which tool is in use. Tools based on object-linking tied to the data's XML description can be synthesized on the spot.

Firewalls

- **Packet filter firewalls** historically implemented on routers, filter on user defined content, such as IP addresses. They examine a packet at the network layer of the **Open Systems Interface (OSI)** model and are application independent, which allows them to deliver good performance and scalability. They are the least secure type of firewall because they cannot understand the context of a given communication, making them easier for hackers to break.
- **Application gateway firewalls** improve on security by examining all application layers, bringing context information into the decision process. However, they do this by breaking the client/server model. Every client/server communication requires two connections – one from the client to the firewall and one from the firewall to the server. In addition, each proxy requires a different application process, or daemon, making scalability and support for new applications a problem.
- **Stateful inspection firewalls** overcome the limitations of application gateways and packet filters by providing full application-layer awareness without breaking the client/server model. With stateful inspection, the packet is intercepted at the network layer, but then the firewall extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. This solution is dramatically

improves on the performance of an application gateway, while offering the same or better security.

G

Gateway – A computing system or software function that performs a protocol or API translation, and serves as an intermediary between computing systems or communications networks.

Geospatial – Information that identifies the geographical location and characteristics of natural or man-made features and boundaries of the Earth.

Geoprocessing – Computer applications which model, interpret and use Earth information.

Granularity – Degree of parallelism in an architecture, from job execution level (coarse) to logic device level (fine). Ability to increase system capacity and performance through incremental processor expansion.

Graphical User Interface (GUI) – facilitates application use by means of windows, icons, and menus

Groupware – or collaborative software, was defined as a new software category by the introduction of Lotus Notes in 1989. Groupware applications support a wide variety of activities, such as e-mail, scheduling, and document sharing. Some groupware products are suites of ready-made applications; others are toolboxes for creating collaborative applications, with customizable templates included. Groupware enables an organization to compile, organize, and share its knowledge base, that is, to perform **computer-supported cooperative work (CSCW)**. The goal of groupware is to enable collaboration by letting team members focus on tasks at hand rather than on the process of gathering and integrating information. Groupware maximizes human interaction while minimizing technology interference. It increases efficiency by decreasing the time and effort expended distributing data files and other documents among working groups and individuals. Groupware provides the infrastructure for groups and individuals to work cooperatively and share information electronically, regardless of where they are located.

Governance – A subset of the Architecture Management processes that are focused on ensuring that IT projects either adhere to the preferred direction set forth in the architecture or are explicitly granted an exception to the principles, standards and products dictated by the architecture.

H

Haptic – Applying tactile sensation and control to interaction with computer applications.

Hardware – The physical entities of an enterprise architecture. A computer with one or more physical network connections.

Hierarchical – An approach used in numerous technologies, including machine vision, process control, networking, databases, and planning, whereby the scope of work is arranged in hierarchies that establish priorities and appropriate routings. A database architecture in which data elements are arranged in the form of an inverted tree structure in which no data element has more than one parent.

Hub & Spoke – A particular architectural pattern where applications and components exchange information and request services via messages through a centralized hub or hubs which route and distribute the messages.

Hubs – Hubs are shared devices that allocate the available bandwidth to all devices attached.

Hypertext Markup Language (HTML) – A world wide web authoring language used for creating and linking Web pages.

Hypertext Transport Protocol (HTTP) – The communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a server and transmit HTML pages to the client browser. Users of the web retrieve documents from servers or "web sites".

I

Information – Structured data.

Infrastructure – An underlying base or foundation supporting an organization or system. Technical infrastructure supports the technical capabilities of business applications and data repositories, and does not contain business specific logic or functionality.

Interface – (1) A shared boundary between two pieces of equipment. (2) The hardware and software needed to enable one device to communicate with another.

An **Interface Definition Language (IDL)** is a generic term for a language that lets a program or object written in one language communicate with another program written in a different language. In distributed-object technology, it's important that new objects are able to be sent to any platform environment and "know" how to run in that environment. An **IDL** within the object-oriented world is fundamentally the same as in the RPC world; however, here it permits interfaces to objects to be defined independent of an objects implementation. After defining an interface in IDL, the interface definition is used as input to an IDL compiler that produces output that can be compiled and linked with an object implementation and its clients, thus allowing for client-server communication across a distributed heterogeneous environment.

Internet – The "Infobahn" of tens of thousands of public and private networks worldwide. The Internet's TCP/IP communications standards mean computers anywhere in the world — even those running different operating systems and applications—can communicate with one another.

Hypertext Markup Language (HTML) lets the computers display the accessed information in graphical pages.

Intranet – Networks within a business using the same technology that is the foundation of the global Internet. Many industry analysts expect such corporate networks to provide most of the revenue for computer hardware and software vendors over the next few years as an increasing number of businesses expand their internal networks to improve efficiency and build closer ties with customers and suppliers.

Interoperability – The ability of computers on a network to share application software.

Intrusion Detection – A process or product for detecting unauthorized entry or access to a computer or network.

IP Security Protocol (IPSec) – A standardized means of implementing security for VPNs. IPSec is a set of **Internet Protocol (IP)** extensions that provide security services at the network level of the OSI stack. IPSec technology is based on modern cryptographic technologies, making possible very strong data authentication and privacy guarantees. Furthermore, all of the encryption and authentication algorithms and security protocols used in IPSec are well studied and have survived years of scrutiny. Consequently, the Bureau can be confident that the IPSec facility indeed provides strong security. IPSec can be implemented in routers or firewalls owned and operated by the IEA. This gives the network management facility complete control over security aspects of the VPN.

J

Java – A programming language based on C, developed by Sun Microsystems that extends and complements the basic capabilities of Hypertext Markup Language (HTML). Originally developed as a language for consumer-oriented devices such as TV set top boxes, Java became a viable alternative to other programming languages with the rapid growth of the Internet as it has the potential to work on an unlimited number of computing devices and operating systems. Java permits the creation of applications and application modules (“applets”) that run in the Java virtual machine (JVM) on the browser, either as software on a PC or on the Sun picoJava chip, a piece of dedicated hardware. Browsers from both Netscape and Microsoft have a JVM. Java’s platform independence and security are designed in, rather than added on, so applications can run on a wide variety of desktop platforms as long as they can run a Java-enabled browser. Principally a programming language, but it has been designed by Sun Microsystems to function as a complete computer operating system. The purpose of the language is twofold – to create a single standard that will run on a variety of competing computer systems, and to solve vexing computer security problems introduced by the widespread reliance on computer networks, which are vulnerable to malicious programs such as viruses.

Java Applets – A small piece of Java code that implements a specific function. Applets may run on a server or be downloaded and run on the client’s machine.

Java Database Connectivity (JDBC) – a standard set of Java classes providing vendor-independent access to relational data.

Java Remote Method Invocation (RMI) – is Java's remote procedure call (RPC) mechanism. It functions only within the Java Virtual Machine (JVM) environment; however, with the Java native method interface (JNI), a developer can connect to existing and legacy systems. It facilitates interprocess and intraprocess communication.

Java Servlets – A form of server-based Java that operates in conjunction with a Web server and offers an alternative to using Common Gateway Interface (CGI) and server application programming interfaces (SAPIs) to communicate with Web server processes. In addition, servlets are independent of a given type of Web server, as the most prominent Web servers support servlets.

Java Transaction Service (JTS) – Controls transaction applications, performs database updates, provides database connection pooling, and provides reliable manageability of client connections within the Java environment.

K

Knowledgebase – Data, including assertions, rules, objects, constraints, or other items, used by an expert system or knowledge-based system.

Knowledge-Based System – Software that uses artificial intelligence techniques and a base of information about a specialized activity to control systems or operations.

L

Local Area Networks (LANs) – span a limited geographical area to connect computers and terminals, usually at moderate-to-high data rates.

Legacy System – Existing systems using older and often outdated technology.

Legal Data – The portion of the enterprise that contains all of the primary data stores required to be maintained by law. Legal data is not necessarily stored in electronic format.

Lightweight Directory Access Protocol (LDAP) – DAP runs over the OSI network protocol stack. That, combined with its very rich data model and operation set makes it difficult to implement a full-blown DAP client and have it “fit” on smaller computer systems. LDAP, however, is, like X.500, both an information model and a protocol for querying and manipulating it. LDAP's overall data and namespace model is essentially that of X.500. The major difference is that the LDAP protocol itself is designed to run directly over the TCP/IP stack, and it lacks some of the more esoteric DAP protocol functions.

Line of Business (LOB) – Individual business unit within a larger organization.

Logical Model – A model depicting a view of something that is independent of the way in which it is implemented physically. A logical view expresses semantics, rules, relationships, and behaviors that are often used as the basis for physical design.

Local Area Network (LAN) – A geographically limited communication network that connects users within a defined area. A LAN is generally within a building or small group of buildings and is managed and owned by a single enterprise. The shorter distances within a building or campus enable faster communications at a lower cost than wide-area networks (WANs). Although an increasing number of LANs use Internet standards and protocols, they are normally protected from the public Internet by firewalls.

Long-Term Direction – Technologies and products that are planned for the time frame ranging from 18 months past the publication date of the TRM to five years beyond the TRM publication date.

M

Message-Oriented Middleware (MOM) – is a layer of code which allows for application communication over a distributed heterogeneous environment. It may employ synchronous or asynchronous communication, some combination as in beginning a session in synchronous mode and falling back to asynchronous if need be. The MOM code is required on the client and the server and ideally should employ message queues which frees both client and server to go about their business without concern for the message being received. This flavor of middleware is best suited for event driven applications involving an occurring event the client application hands off to the messaging middleware the responsibility of notifying a server that some action needs to occur.

Message Transfer Agent (MTA) – An e-mail delivery application that receives messages from an MUA or another MTA, stores them while it determines where and how they are to be delivered, and delivers the messages to individual addressed mailboxes or other MTAs. Transferring an e-mail message from the composition area to the e-mail server requires that an MTA communicates via the same protocol (or language) as the server. The three most commonly used protocols are Post Office Protocol (POP) and Internet Message Access Protocol (IMAP), which define methods for e-mail clients to retrieve messages from a server on a TCP/IP network; and the Internet Simple Mail Transfer Protocol (SMTP), the Internet e-mail standard used to deliver messages between servers connected to the Internet.

Messaging – the standard means for executing interprocess communication facilitated by middleware technologies. (See the Middleware Architecture chapter of the TRM.)

Metadata – information about data, including the format of the data element, which application system owns it, where it is located, and how it should be used. Metadata is the global information about what data exists across the enterprise and the standards applying to that data. It is very

important to the data warehouse effort because it sets the standards and the rules used for data transformation and cleansing.

Middleware – connectivity software that consists of a set of enabling services that allow multiple processes running on one or more machines to interact across an environment. Middleware is essential to migrating mainframe applications to client/server applications and to providing for communication across heterogeneous platforms.

Mirroring – Writing duplicate data to more than one device (usually two hard disks), in order to protect against loss of data in the event of device failure. This technique may be implemented in either hardware (sharing a disk controller and cables) or in software. It is a common feature of RAID systems.

Module – A separate and distinct unit of hardware or software.

Monitoring Tools – Tools used for monitoring a system's real-time availability and performing statistical analysis on the results of the monitoring.

End users access a multidimensional database through a query language called **Multidimensional Structured Query Language (MDSQL)**. MDSQL is the multidimensional database query language, just as SQL is the query language for a relational database. However, where SQL has an industry standard called ANSI Standard SQL, there are no current industry standards for MDSQL.

Multimedia – Integration of text, voice, video, images, or some combination.

Multiplexer – Electronic equipment that allows two or more signals to pass over one communications channel.

N

Near-Term Deployment – Technologies and products that are planned for the time frame ranging from the TRM publication date to the TRM publication date plus 18 months (full deployment within 18 months).

Network Architecture – The Network Architecture provides the communication infrastructure for the distributed computing environment. It consists of logical elements (structure, topology, bandwidth, management), physical hardware components (wiring, LANs, hubs), carrier services (frame relay, leased channels, ATM), and protocols (access routing, naming).

Network Connection – A network connection is a peer to peer, software, bidirectional connection between two applications. The TCP/IP protocol is the most common network protocol in use today. Data transmitted via TCP/IP is byte-aligned and is streamed. Applications receiving data via TCP/IP may receive as little as one byte at a time. Applications that use streaming network protocols must parse the data stream to understand it.

The **Network File System (NFS)** uses either TCP/IP or UDP protocols for sharing disk space from one system among other systems.

Node – One component of a network where interconnections occur.

N-tier architectures – Some systems take the partitioning of applications one step further and split one or more of the tiers across the network. For example, a distributed database service enables an enterprise's database to run on multiple types of machines and still present a logical view of a single database to the application logic that accesses the database. A distributed function service allows the middle tier that runs the business logic to be partitioned and run on multiple machines. In such cases, the partition points are not just at the presentation /logic or logic/data boundary. Partitioning can occur almost anywhere inside the logic or data section. Physically, the application can run across four, five, or even more machines (tiers); hence the term N-tier, where “N” equals any number.

O

An **Object** is a self-contained bundle of software with an identity that is unique among the objects in a system. Each object consists of **variables** that store data and **methods**, or procedures, capable of acting on the object's variables. The object encapsulates its variables, and it is only through sending message to the object's methods that another object can access the contents of the variables. Variables can be numbers, character strings, or other data types. In addition to its variables, an object contains **methods**. These are the procedures that enable other objects to access variables and perform operations on them. The main mechanism for bring order to objects is the **class**. A class is a template for objects, which contains the methods we want our object to have plus data-type definitions for its variables. Objects are instances of classes.

Object Linking and Embedding (OLE) – A Microsoft protocol that enables creation of compound documents with embedded links to applications, so that a user does not have to switch from one application to another to make revisions. The following are features of OLE:

- Users can create compound documents using multiple applications
- Compound documents may contain text and spreadsheet objects, graphic and chart objects, sound objects, and video and animated objects
- Objects that support OLE automation may be scripted by OLE controllers, such as Visual Basic, and used in end-user-developed applications.

Object-Oriented Database – A database used to store objects that form the basis of object-oriented computing, in which data, as well as references to the procedures used to perform operations on that data, are combined.

Object-Oriented Design (OOD) – A design method in which a system is modeled as a collection of cooperating objects and individual objects are treated as instances of a class within a class hierarchy. Four stages can be identified: identify the classes and objects, identify their semantics,

identify their relationships, and specify class and object interfaces and implementation. Object-oriented design is one of the stages of object-oriented programming.

Object-Oriented Programming – Programming based on objects that communicate by passing messages. An object is a package of information and descriptions of procedures used to manipulate that information.

Object-Oriented Software – Results from a kind of modular programming. Each object is a software package containing a collection of related procedures and data that can be reused to shorten application development time. Objects also make it easier to customize software systems to mirror actual business processes without negatively impacting the ability to migrate to later software releases.

Object Request Broker (ORB) – Middleware that allows objects to communicate within a distributed environment.

Online Analytical Processing (OLAP) – 1) Enables a user to easily and selectively extract and view data from different points-of-view. To facilitate this kind of analysis, OLAP data can be stored in a multidimensional database. A multidimensional database considers each data attribute as a separate dimension. OLAP software can locate the intersection of dimensions and display them. Attributes such as time periods can be broken down into subattributes. OLAP can be used for data mining or the discovery of new relationships between data items. OLAP data is often stored in data warehouses and data marts (i.e., a specialized subset of a data warehouse). An OLAP database does not need to be as large as a data warehouse, since not all transactional data is needed for trend analysis. 2) Online analytical processing is a process where many system users are retrieving data from a data store for analysis.

Online Transactional Processing (OLTP) – 1) A class of program that facilitates and manages transaction-oriented applications, typically for data entry and retrieval transactions. Today's online transaction processing increasingly requires support for transactions that span a network and may include more than one government organization. For this reason, new OLTP software uses client-server processing and brokering software that allows transactions to run on different computer platforms in a network. 2) Online transaction processing is a process where many system users are creating, updating, and deleting data in a data store via one or many applications. This process is commonly referred to as CRUD, for create, update, and delete.

Open Database Connectivity (ODBC) Drivers – the middleware used to connect database access tools to relational databases through the use of a generic API. ODBC drivers are vendor-provided and allow databases to be connected and used by a generic interface. The ODBC drivers enable access to data and provide insulation between a program and the specific RDBMS language used by each database. Database access tools and programs do not have to be customized for each database, because an ODBC configuration file maintains the database connections.

Open Systems – An approach to computing that stresses the interconnectability of systems based on compliance to established standards.

OSI (Open Systems Interconnection) – International standardization program, facilitated by ISO and CCITT to develop standards for data networking, which facilitates multivendor equipment interoperability.

Operating System – A structured set of system programs that controls the activities of a computer system and associated peripheral devices, as well as the execution of programs and flow of data.

Operations Management – Encompasses the back office component of systems management, focusing on practices for delivering available systems with adequate responsiveness. Functions include software distribution, storage management (including systems backup and recovery, server performance monitoring and tuning, software license management, user administration and account management, etc.)

Operational Data Store – A subject-oriented, integrated, single source and up-to-date collection of data used to support the tactical decision-making and day-to-day information needs of the business. The data primarily comes from a replicated copy of disparate Core Business Operational legacy data that is updated in a timely manner (i.e. near real-time up to 24 hour latency). The data needs to be 100% accurate and should meet the performance requirements (i.e. typically OLTP and operational reporting processing) set by the business.

OSI Reference Model – Network architectural model developed by ISO and CCITT. The model consists of seven layers, specifying network functions such as addressing, flow/error control, and encapsulation.

P - Q

Partitioning – Applications can be broken into three logical parts: presentation, logic, and data. These are areas in which the program can be separated to facilitate execution of each logical piece on a different machine. Each segment is known as a partition. For example, the thin-client Web model requires that interface presentation be handled by the browser, application logic by the World Wide Web server and other application servers, and data by a database server. Developers are responsible for determining where the separation occurs. Early client/server applications used architectures dictated by the tools employed in their construction. As a result, most of the early applications used a two-tier client/server architecture. The tiers of client/server applications refer to the number of executable components into which the application is partitioned, not to the number of platforms where the executables are deployed. Sometimes the tiers into which the application is partitioned is called **logical partitioning**, and the number of physical platforms on which it is deployed is called **physical partitioning**.

Personal Digital Assistant (PDA) – A handheld, wireless computer that serves as an organizer, electronic book or note taker. It typically uses a stylus or pen-shaped device for data entry and navigation.

Physical Model – A model used to depict how data is physically implemented. It should include the physical names, data types, dependencies and relationships to other data.

Plug-in – An application used within another application to extend its functionality.

Portal – An entry point that collects relevant information to support a theme or service.

Post-Relational Database – A new class of database that combines the speed and scalability of a transactional multidimensional data model with the power and flexibility of object technology. Because of their unique capabilities, post-relational databases are ideal for developing high-performance transaction processing applications.

Presentation Layer – This is the front-end client that communicates with the user through an interface. Good architectural designs ensure that the presentation of an application is separated from the business logic. This ensures that an application can have many presentations depending on user needs (i.e. Web, internal client interface, voice response system, other systems). Changes in the presentation are easily made without effecting the underlying business application.

Principles – *Guiding* statements of position that communicate fundamental elements, truths, rules, or qualities that must be exhibited by an enterprise. Statements of *preferred* architectural direction or practice that provide a context for architectural decision-making. They identify desired behaviors and eliminate the need for evaluating endless alternatives through advance agreement on preferred direction.

Program – (1) A complete, structured sequence of program statements directing a computer to implement an algorithm. (2) All software programming necessary to solve a problem.

Programming Language – An artificial language that enables people to instruct machines. Computer commands that form procedures by which software programmers design and implement computer software programs.

Protocol – A standard set of procedures that allows data to be transferred among systems.

Proxy Servers – Devices that process and filter all Internet Protocol (IP) packets that are directed to them and decide which protocols and services can be served out of their caches. Proxy servers tend to offer the greatest range of protocol and caching support since they cache Hypertext Transport Protocol (HTTP), Secure Hypertext Transport Protocol (HTTPS), File Transfer Protocol (FTP) and, in some cases, streaming content such as RealAudio and PointCast. Each workstation addresses the proxy server directly by setting specific parameters in each browser on each workstation.

Public Key Infrastructure – The process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person

who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it

Push Technology – Software that automates the delivery of information to users. In contrast, the World Wide Web is a “pull” environment that requires a user to seek information. In a “push” environment, information is sent to a person proactively, through a Web browser, e-mail, or even voice mail or a pager. In business, push technology can be used for the conveyance of time-sensitive information, like changes in commodity pricing or the introduction of promotional programs to a sales force. Enterprises can employ push technology to communicate externally with their clients or internally with their employees over a network.

Query – A request for data that is initiated while a computer program is running.

R

Rapid Application Development (RAD) – An application development (AD) approach that includes small teams (typically two to six people, but never more than 10) using joint application development (JAD) and iterative-prototyping techniques to construct interactive systems of low to medium complexity within a time frame of 60 to 120 days.

Recommended Best Practices – Very specific recommended actions that will aid in the successful implementation of architectural elements covered in the IT Technical Reference Model. Usually expressed as simple declarative sentences. For example, “Use font sizes large enough to be read on standard size monitors”.

Redundant Array of Independent Disks (RAID) – A method of mirroring or striping data on clusters of low-end disk drives; data is copied onto multiple drives for faster throughput, error correction, fault tolerance and improved mean time between failures. With the exception of RAID 0, all RAID levels provide automated recovery of data in the event of a disk failure. The RAID levels and their key features are as follows:

- **RAID-0** – provides disk striping without parity information; data is written by segment across multiple disks sequentially until the end of the array is reached, and then writing starts at the beginning again. Provides greater logical disk capacity with faster access time on reads (multiple segments read simultaneously). However, RAID-0 provides no data redundancy – if one drive fails, the entire disk array subsystem is unavailable.
- **RAID-1** – provides fault tolerance by using disk mirroring (also called shadowing). Each byte of data on a disk is duplicated on another physical drive, providing 100-percent data redundancy. RAID-1 provides immediate access to data when either the primary or secondary drive fails, but it has the highest cost of all RAID types, since duplicate hardware is required.
- **RAID-2** – eliminates the 100-percent redundancy overhead of RAID-1 by using a powerful error detection and correction code (Hamming), with bits of the data pattern written across multiple disks.

- RAID-3 – similar to RAID-2, but uses a single check disk per group that contains the bit parity of the data disks; data is interleaved across all disks. Because disk reads are performed across the entire array and all data is transferred to the controller in parallel, RAID-3 is well suited for applications that require high data read/write transfer rates for large sequential files.
- RAID-4 – instead of interleaving blocks of data across all drives, writes the first block on drive 1, the second block on drive 2, and so on. This technique dramatically improves read time, since many reads are single block (single drive), freeing other drives for additional read requests.
- RAID-5 – eliminates the dedicated parity drive by writing parity with the data across all drives in the array. Consequently, the single-write restriction and some performance degradation of RAID-1 through RAID-4 are eliminated. If a drive fails, the controller can rebuild the data from the parity and data on the remaining drives.
- RAID-6 – provides two-disk parity and one spare, so that two simultaneous disk failures per array of disks can be tolerated. With the occurrence of a failure, a spare is brought online and transparent reconstruction begins automatically in the background with negligible impact on performance.
- RAID-10 – a combination of RAID-0 and RAID-1 that provides the benefits of striping and fault tolerance (disk mirroring).

Relational Database Management System (RDBMS) – A database management system (DBMS) that incorporates the relational-data model, normally including a Structured Query Language application programming interface. It is a DBMS in which the database is organized and accessed according to the relationships between data items. In a relational database, relationships between data items are expressed by means of tables. Interdependencies among these tables are expressed by data values rather than by pointers. This allows a high degree of data independence.

Real Time – Response to events in a predictable and immediate way. A spreadsheet response in one second or five seconds is acceptable, but closed-loop control systems need to know real-time response rates in a more rigorous manner.

Real-Time System – Computers designed to receive, process, and respond to data within a time frame set by outside events, e.g., for air traffic control. A system consists of a controlling system and a controlled system. A controlling system interacts with its environment based on information from various sensors and inputs. In many real-time systems, severe consequences result if the timing and logical correctness of the system are not satisfied.

Relational Database – A DBMS in which the data is perceived by the user as a collection normalized relations of assorted degrees.

Remote Access Technology – a method for providing traveling or homebound users within the IEA with access to the data networks of the Bureau. Remote access is usually designed to support communications from home to mainframes, LANs, e-mail, UNIX systems, and minicomputers.

Remote Procedure Call (RPC) – A mechanism that extends the notion of a local (i.e., contained in a single address space) procedure call to a distributed computing environment, enabling an application to be distributed among multiple systems in a way that is highly transparent to the application-level code. Examples of RPCs are Sun Microsystems' Open Network Computing, Sybase's Open Client/Open Serve and the Open Software Foundation's Distributed Computing Environment (DCE) RPC.

Replication – Creating and maintaining a duplicate copy of a database or file system on a different computer, typically a server. The term usually implies the intelligent copying of parts of the source database that have changed since the last replication with the destination. Replication may be one-way or two-way. Two-way replication is much more complicated because of the possibility that a replicated object may have been updated differently in the two locations in which case some method is needed to reconcile the different versions.

Replication Services – When databases are geographically distributed, they are kept up to date from a central source database through replication. Replication services propagate data and transactions that occur in a central source database to each participating remote database.

Reporting Tool – Technologies used for complex reporting using DBMS data.

Repository – Passive data dictionary or encyclopedia that offers a single point of definition for all application components.

Repudiation – Repudiation is the act of refusing to receive or acknowledging receipt of a security authorization request. Non-Repudiation is the security concept that protects "against denial of sending (or receiving) a data item by the sender (or recipient).

Requirements for Technical Architecture – The capabilities that the technical architecture must provide in order to satisfy the business information requirements.

Router – Network device used to Interface between two networks. Routers work at the Network layer of the Open Systems Interconnect (OSI) reference model.

Rules-Based System – A functional system in which knowledge is stored in the form of simple if/then or condition/action rules.

S

Scalable – Able to meet demands for increased performance, processing power, network connectivity, and data storage.

Search Engine – A program used for the cataloging and indexing of web content for the purpose of locating desired information.

Security Architecture – The Security Architecture defines the components and functions necessary to ensure that the organization's systems, applications and data are secure from internal or external tampering and unauthorized. It takes into consideration the functions of authentication, authorization, encryption, access control, message integrity, non-repudiation and auditing.

Security Services – These services include operational methods necessary to enable authenticated user access to systems and data, virus detection methods to minimize risk to system integrity, methods to permit remote access for trusted users, methods to enable on-site access to untrusted users through IEA public rooms, and methods for off-site access to public information available on IEA systems.

Services – In an N-tier service-oriented architecture, applications are partitioned into discrete units of functionality called services.

Server – A processor that provides a specific service to the network. In a client/server architecture, servers perform central storage and other vital tasks. Servers specialize in high-speed computation and data storage and manipulation. They can range in size from PCs to mainframes.

Service Level Agreement (SLA) – Contract service definition, stipulating how service/product delivery or consumption is to be performed and measured.

Session – A period of continuous interaction between and user agent and a server.

Shared Data – data available for use both within the Bureau and between multiple governmental organizations. When shared data is used, it is stored and maintained once. It can then be accessed by each system that needs it. Application systems do not have to duplicate any efforts to collect, verify, store, and maintain data used by multiple application systems, whether the application systems run in a single location or in multiple locations across the Bureau.

Simple Mail Transfer Protocol (SMTP) – The standard for sending mail to and from the Internet.

Simple Network Management Protocol (SNMP) – A Transmission Control Protocol/Internet Protocol (TCP/IP)-derived protocol governing network management and the monitoring of network devices.

Software – Code, data, and documentation maintained in a specific configuration. The entire set of programs, procedures, and related documentation associated with a computer.

Source – A place from which data is taken. Data is taken from a source, whereas the place it is moved to is called the destination or target.

Spatial Data Servers – have emerged in a three-tier database architecture that provides a comprehensive GIS solution. They provide an open interface between the user and all of the geographic information in an organization. With this type of spatial data server architecture, data can be delivered to any client, from any server, anywhere on the network (within network performance constraints).

Steward – One who has been assigned the responsibility to provide day-to-day (operational/tactical) support and manage the interests of a given data subject area, application area, technology, process, business unit, organization, or asset, or who as a representative would be impacted by change to these same interests.

Stove-Piping – Building systems that do not interoperate or collaborate with each other (e.g., unable to share data or application modules).

The **Structured Query Language (SQL)** is used to query and retrieve data from relational databases. Allows a client to access only the data required to satisfy a request for data, cut network traffic, or improve performance. An accepted standard that most relational database products implement. The industry standard for SQL is ANSI Standard SQL. SQL drivers are implemented by each RDBMS vendor to enable database access to its proprietary database. Vendors may add extensions to the SQL language for their proprietary databases. SQL provides an implementation for data retrieval from an RDBMS. The use of SQL requires knowledge of the physical data store.

“Strong” Passwords – A strong password will consist of at least eight characters, contain a minimum of one capitalized letter; one lower case letter, one numeric character, and one special character (such as !@#\$%^&*+=, etc.). Therefore, a password such as J0hN^4sM1th, although still somewhat easy to remember, will require a brute force password-guessing program that might take several days to crack the password. An intruder who fails to guess a password rapidly will probably abandon the effort to avoid detection.

Switches – A network device working at the Data Link layer of the OSI model. A switch has the same function as a bridge.

Synchronous media, where participants in computer-supported communication meet at the same time, and **Asynchronous** media, where participants connect at different times and leave files and messages for others to read and comment on. By way of example, telephony is considered to be synchronous, while e-mail, often used for the same purpose, is asynchronous.

System – A system is composed of one or many applications executing against one or more data stores.

Systems Management – Coordination and maintenance of all software on a client/server network, including performance monitoring, applications distribution, version control, user administration, job scheduling, data backup, security, and configuration management.

System Development Lifecycle (SDLC) – An SDLC provides an established procedure to approach the technical aspects of a project. It provides technical definition based on a phased sequential approach to systems development. The intent of the SDLC project breakdown is to define a logical, sequential group of activities and deliverables that lead the team through the project phase by phase.

The **System Services Layer** encompasses the operating system, networking software, system management, file system, database services, UI (user interface) library, and so on.

T

T1/T1C/T2/T3/T4 – A digital carrier system introduced by the Bell System in the United States in the 1960s. It was the first to successfully support DS-1 formatted digitized voice transmission that connected directly to a network. T1 and T3 lines are often used in Internet service provider (ISP) connections to the Internet. T-series speeds include: 1. T1: 1.544 megabits per second (Mbps) 2. T1C: 3.152 Mbps 3. T2: 6.312 Mbps 4. T3: 44.746 Mbps 5. T4: 274.176 Mbps.

Technical Architecture – the strategy and standards for utilizing technology tools. The Technical architecture defines the capabilities for loosely coupling components to service a business process.

Three-Tier Hardware Architecture – involves three classes of machines. The client is usually a PC; the middle tier is usually a workstation server or a minicomputer; the back end is usually a mainframe. **Two-tier hardware architecture** generally involves only the client and either a middle-tier server or a mainframe.

Thin Client – Since the major components of a distributed object application are located on a server (or a network of servers), the client-side application can be kept small and lightweight (that is, “**thin**”). This allows more of the clients' system resources to remain free while the bulk of the application processing is performed on the high-end servers.

Three-Tier Client/Server Model – Current IEA development uses a three-tier client/server model. The first tier is the Web server layer where the user interface resides. The second tier is the application server layer where the business rules reside. The third tier is the database server layer where the data resides. Three-tier client/server applications offer the following advantages: Three-tier client/server applications can be easier to modify to support changes in business rules; with three-tier client/server applications there is less risk in modifying the code that implements any given business rule; three-tier client/server applications can be made to support multiple user interfaces (character, graphical, Web browser, telephones, etc.)

Topology – The physical layout of a network, including the method of connection between nodes on the network.

Trade Studies – Requirements exist for technologies or products that must be chosen based on business requirements and selection criteria.

Transmission Control Protocol/Internet Protocol (TCP/IP) – The Internet’s communication standard. It allows different types of computers to share data on a network. Every transmission gets broken down into standard-sized packets, like little envelopes of data. Each packet carries an address, but no information about what is inside. A set of protocols covering (approximately) the network and transport layers of the seven-layer Open Systems Interconnection (OSI) network model. TCP/IP was developed during a 15-year period under the auspices of the Department of Defense. It has achieved de facto standard status, particularly as higher-level layers over Ethernet. TCP/IP implementations are available on products from more than 80 vendors, including IBM, Digital Equipment, AT&T, Data General and Sun Microsystems. The biggest issue for TCP/IP is potential migration to the International Standards Organization (ISO) protocols for Layers 3 and 4.

Trusted User – A user that has full access to all of the resources that the user requires. A trusted user can be a IEA employee or an employee of another agency such as the Forest Service that has access requirements (**External Trusted User**).

In a **Two-Tier Client/Server Architecture**, application functionality is partitioned into two executable parts, or tiers. On one model, one tier contains the code that implements a graphical user interface (GUI) and the code that implements the business rules. This tier executes on desktop workstations and requests data from the second application tier, which usually executes on the machine where the application's data is stored. This model is referred to as two-tier, **fat client** because, while the application is partitioned into two tiers of executable code, most of the application's code is contained in the tier executing on the desktop workstation, the fat client.

U

Unified Modeling Language (UML) – A de facto standard notation for modeling objects.

Untrusted User – Any user not granted access to IEA’s internal network. Includes the public.

Usability – A system can be said to be “usable” when specified users, in specified circumstances, with specified goals, can use it with effectiveness, efficiency and satisfaction. Improving usability can be accomplished by applying practices and techniques that help understand and meet the needs of users.

Utility – A [program](#) that performs a very specific task, usually related to managing [system resources](#). [Operating systems](#) contain a number of utilities for managing [disk drives](#), [printers](#), and other [devices](#). Utilities differ from [applications](#) mostly in terms of size, complexity and function. Utilities are sometimes installed as [memory-resident](#) programs.

V

VBScript – A primary form of Microsoft’s Visual Basic (VB). It has been introduced as Internet-oriented scripting language intended for providing client-side and server-capable processing within Web pages.

Very Large Database (VLDB) – A database which contains 50 million rows or more.

Video Conferencing – systems that allow two-way or multi-way calling with live video, essentially a telephone system with an additional visual component.

Virtual Private Network (VPN) – A network that is constructed by using public wires to connect nodes. A VPN is a way of using a public network transport to form a secure network connection, either between two enterprise sites (LAN to LAN) or between an individual and a site (PC to LAN). The purpose of a VPN is to allow an organization such as the IEA to extend its network trust perimeter over the public network without sacrificing security. Using the Internet as a backbone, a VPN can securely and cost-effectively connect IEA telecommuters, mobile workers, and external customers (such as the USFS or MMS).

Visual BASIC for Applications (VBA) – A Visual Basic system included with Windows 95 applications and used for creating basic and customized programs.

Voice Mail – A messaging tool that receives and stores voice messages as well as serves as an automated attendant to route incoming calls and messages.

VoiceXML (VXML) – A high-level programming language able to handle text-to-speech applications, output of audio files, and recognition of spoken input.

W

Web Authoring Tools – A development environment used to create web content.

Web Browser – A program used to view, download, upload, and access documents via Internet protocols. The scope includes both browsers supported internally for intranet users, and browsers supported externally for Internet users.

Webcasting – (1) Delivery of a transmission to two or more “stations” at the same time, such as over a bus-type local network or by satellite. (2) Protocol mechanism whereby group and universal addressing is supported.

W3C – World Wide Web Consortium.

White Boards – are a real-time technology that allows two or more people to view and draw on a shared drawing surface, even from different locations. It can be used for brainstorming and summarizing ideas, or to work collaboratively on a visual problem, just as with a standard white

board. Most shared white boards are designed for informal conversation, but they may also serve structured communications or more sophisticated drawing tasks, such as collaborative graphic design, publishing, or engineering applications.

Wide Area Network (WAN) – A communications network that connects computing devices over geographically dispersed locations. While a local-area network (LAN) typically services a single building or location, a WAN covers a much larger area such as a city, state or country. WANs can use either phone lines or dedicated communication lines.

Wiring – Low voltage cabling used to connect network devices at high frequencies.

Workstation – A single-user computer, typically with 32-bit messaging and integrated graphics.

Workflow Software – Software that automates an enterprise’s business processes (i.e., the sequence of actions, activities, or tasks used to complete a business process) and tracks their status (the status of each instance of the process). Work can be assigned, routed, activated, and managed through system-controlled rules that mirror business operations and decision processes.

World Wide Web (WWW) – Internet system for hypertext linking of multimedia documents, allowing users to move from one Internet site to another and to inspect the information that is available without using complicated commands and protocols.

Wrappering – A process whereby legacy applications can be formed into components by implementing code (i.e., a “wrapper”) that “wraps” an API around a legacy service

X– Z

The **X.500 Directory Service** provides a lookup of names and addresses through the **Directory Information Base (DIB)**. It is a specification for global directory servers and access. It was designed to work with the old X.400 directory service and other message handling services. Each object stored in the DIB is grouped within an hierarchy wherein common name objects are nested within organization-unit objects (for example, “Finance Department”), which are, in turn, nested organization objects (for example, “Nuts and Bolts, Incorporated”). X.500 is an overall model for directory services that encompasses the overall namespace and the protocol for querying and updating it. The protocol is known as **“Directory Access Protocol” (DAP)**.

XML (Extensible Markup Language) – is used to provide structure to data. For example, a water sample is extracted from a stream and its temperature is measured as 12 Celsius. The measurement 12 is the data while many other attributes of the measurement need to be recorded. The units of measure (Celsius), the location of the measurement, the flow rate of the stream, the specific type of thermometer used for the measurement, the identification of the analyst and the clarity of the water sample are possible attributes to record with the sample temperature. Recording the attributes with the temperature results in the creation of information from the temperature datum. XML provides a standard mechanism for structuring and recording data so that it can be shared and understood by many systems and by people. XML uses plain text instead of

binary encodings. XML is self-describing. XML uses data type definition (DTD) files to describe the format of the XML. Applications can understand each other's XML by exchanging DTDs. XML is maintained by the World Wide Web Consortium (W3C).

X/Open Systems Management (XSM) Reference Model – defines the required management interfaces and describes the components and architecture required to build a comprehensive distributed systems